Secure Collection of Event Logs

The importance of consolidation, correlation, and detection
Enterprise Security Series
Abstract

The purpose of this document is to help users implement a secure method to collect event logs from Windows and other systems over the network.

Many enterprises require collecting and consolidating event logs from different domains or geographical locations. In such cases, the need for secure communications is required at many times. If one depends on the vendor to provide secure means for collection, then it means that the system administrator cannot use his existing expertise but have to train himself on new methods. Also, the admin will now depend on one more party to provide for regular updates and training.

Today's Windows systems are rich in the support for secure communications. It is therefore, ideal if the admin can use the existing Windows infrastructure itself to provide for secure communications.

This paper talks about an easy method to collect event logs securely.
# Table of Contents

Secure IP in Windows ........................................................................................................................................... 3  
EventTracker Client System IPSec Setting ................................................................................................................ 25  
  IP Filter Rule Settings ..................................................................................................................................... 25  
  Verify the Settings ............................................................................................................................................ 26  
  Deployment Notes ............................................................................................................................................. 27  
Summary ............................................................................................................................................................. 29
Secure IP in Windows

Starting Windows 2000, secure IP transmission protocols have been introduced in the Windows Operating System. These include protocols such as IPsec which are open standards based on IETF RFCs.

IPSec is a collection of protocols introduced by the IETF and is part of the charter for IP security. We will concentrate on IPSec in this paper as one of the easier methods to achieve the goal of secure event log collection.

Windows gives a flexible IPSec framework where one gets to choose the encryption algorithms, the deployment granularity as well as the certification methods to ensure secure network traffic.

Encryption algorithms provided by Windows include IKE (Internet Key Exchange), ISAKMP (Internet Security Association and Key Management Protocol), MD5, 3DES, SHA-1 and others.

Authentication methods for IPSec in Windows specify how trust is established between two computers. One can choose from Kerberos, Certificate Authority or just a Pre-Shared Key.

Windows provides both the IPSec operation mode settings and that can be one of transport mode or tunnel mode. In transport mode, only the payload of the IP packet is encrypted while in the tunnel mode, the payload and the header of the IP packet is encrypted. The difference between the two is higher security in tunnel mode but at the cost of routing performance.

Finally, the granularity of IP security can be controlled by applying the secure mode operation on only certain flows such as only among a certain subnet of IP addresses or controlled by the Port on which the traffic is sent or received. The type of IP traffic flow can also be specified in terms of ICMP, TCP or UDP as well.

The number of configurable options provided by Windows for IPSec allows an administrator to choose the security level for each of his operations. For example, the flow between clients and server within a private network can be configured on a lower setting than the flow in a public network.

With this background, we will see how to configure an IPSec setting in Windows to secure a specific IP flow between two systems.
Apply IPSec for Secure Collection of Event Logs

This section will talk of how to apply the IPSec principles in securely collecting event logs. For this, we will take the EventTracker product as an example. These principles can be extended to secure any other IP flow in the enterprise.

EventTracker consists of a Client that collects event logs and transfers them to the Manager. The Manager then processes and consolidates these event logs. The transfer between the Client and the Manager can occur on both UDP (hi-performance mode) as well as TCP (guaranteed delivery). For both modes of transfer, the port used is 14505.

The following set of screenshots will now describe the IPSec settings on both the Client system as well as the Manager system that will secure the event log data flow.

EventTracker Manager System IPSec Settings.


2. Configure the name of the policy and the description. Click Next.
3. Leave the default settings, and then click **Next >**.
4. Select the appropriate authentication mode.

   In this case, we have selected a simple mode, which is a simple key exchange.

5. Click **Next >**.
6. Select to **Edit Properties** and click **Finish**.

Selecting a simple key exchange is a good compromise between needing security and having a more complex authentication mode such as Certificate Authority. Choose according to need.
The screen is shown as below with default settings.

7. Click **Add**.
The Security Rule Wizard is brought up for actual port configuration.

8. Click **Next**.
Choose the default setting and do not specify IPSec tunneling.

9. Click **Next >** to continue.
10. Choose appropriate settings.

By default, ‘All Network Connections’ is selected.

11. Click **Next**.
Create the rule for authentication. Here, we choose the simple key exchange protocol.

12. Select Next > to continue.
13. Select **All IP Traffic** and edit the properties.

   You may also want to add a new Filter and keep the default options.

14. Select **Edit**...
After editing All IP Traffic, it can now be changed to describe as EventTracker traffic and relevant description.

15. Select Add to create IP Filter.
The new IP Filter rule wizard is brought up.

16. Click Next >.
17. In **Source Address**: drop down, select **Any IP Address**.

   In this case, we are saying that all the EventTracker agents connecting to the Manager should be using IPSec. The Source Address here is the source address of the Agents.

18. Click **Next >**.
19. In **Destination address**: drop down, select **My IP Address**.

In this case, we are saying that anybody connecting to this system's EventTracker Manager needs to use IPSec.

20. Click **Next**.

21. Select **UDP**, if you are using the default UDP based hi-performance mode for EventTracker operations.

22. Select **Next** to continue.
23. Select the port used by EventTracker.

The settings given below imply that any agent sending information to the local system on port 14505 will be secure.

24. Select **Next >**.
25. If you need to edit or change any properties, select **Edit** and **Finish**.

(OR)

Select **Finish**.

![Image of IP Filter Wizard]

**Figure 17**

The configuration is now updated so that any IP traffic coming to UDP port 14505 is going to be encrypted using IPSec.

26. If any changes are required, select **Edit...** and change. Select **OK** to save the configuration.
We have now configured the rule that we set out doing from Step 11.

27. Click **Next >** to continue.
28. Select IPSec operation mode.

These settings are used to know how the system needs to interoperate with non-IPSec aware systems. Please configure as per need. In this example, the default Request Security policy is chosen.

29. Select Next.
This step establishes the IPSec Rules for the EventTracker Manager system.

30. Select **Edit** to change any settings. Select **Finish** to complete the configuration.
The new rule showing the IPSec settings for EventTracker Traffic on the Manager system is shown.

31. To save, click Close.
The final step requires you to right-click the rule and Assign. The policy should be shown as Assigned.

32. Right-click on the policy and select Assign.
EventTracker Client System IPSec Setting

The EventTracker Client IPSec settings are very similar to the Manager IPSec settings.

The configuration will change only in the IP Filter Settings as given below. All other steps are as given in the Manager System settings. Remember to Assign Policy as well.

IP Filter Rule Settings

The addressing will be configured as **Source=My IP Address** and **Destination=Any IP Address**.

Also cross-check the port settings as given below.
Verify the Settings

Now that the configuration is done, we need to know that everything is working. Microsoft has taken pains to provide a utility that will check for this. The utility is called ‘ipsecmon’ and is available by default on Windows 2000.

The IPSec connection information will be shown as given in this ipsecmon screen which was run on the EventTracker Client system. Here, the policy setting was done on the client system ‘jenniffer’ which is connected to EventTracker Manager system ‘HAGAR’.
In order for the IPSec entry to come up on the screen, there should be traffic between Client and Manager and a delay of at most 1 minute should be allowed.

**Deployment Notes**

In the given example, we use the Shared Key authentication scheme and the Non-Tunneling mode of operation.

Shared Key authentication has been chosen as a compromise between a more secure mode (meaning more overhead) against the overhead of administering something like Kerberos and Certificate Authorities. This trade-off becomes significant when we realize that IPSec being an open protocol can also be used to gather events securely from Firewalls, Routers and UNIX systems through SYSLOG messages or SNMP Traps.
A Shared Key is as secure as a password and hence just like any other password protection scheme, it should be changed at regular intervals to make things life difficult for a hacker.

Non-Tunneling mode has been chosen again for similar reason to that of Shared Key. In addition, due to the tunneling mode of operation, traffic may get slower due to the encrypted IP header being decrypted often for routing purposes.

Having said this, the user needs to understand his deployment and these two trade-offs need not apply to a specific business scenario.

The user also need not have IPSec configured from all Clients to the EventTracker Manager. One suggestion would be to configure IPSec only on Clients being deployed at places away from the base network or subnet. Again, the user is the best judge of this and can decide depending on the requirement.

Lastly, in this example, we have only configured EventTracker for clients sending events through UDP Port 14505 uni-directional from Client to Manager. For securing the TCP mode of operation (guaranteed event delivery), you need to configure for TCP Port 14505 uni-directional from Client to Manager. Also, for securing Client Configuration for remote access, you need to configure for TCP Port 14506 bi-directional.
Summary

Collecting and consolidating event logs is a requirement for most companies now. In many scenarios, the administrator needs to connect to networks that are not in his own subnet or domain. The attention naturally will need to go towards how to collect this important event log information in a secure manner.

This article has proposed a solution to overcome this issue in a non-vendor dependent manner by simply using the existing Windows and other platform infrastructure, in this case IPSec.

The author is a Product Architect at Prism Microsystems, Inc and is responsible for the server monitoring program suite. For further discussion on this topic, interested persons can email support@eventtracker.com.

For further reading, we would recommend the following white papers and technical articles.

2. The IETF charter on IPSec at http://www.ietf.org/html.charters/ipsec-charter.html